

Ist Verkehrssicherheit berechenbar?

Schnieder, Eckehard

Veröffentlicht in:
Jahrbuch 2004 der Braunschweigischen
Wissenschaftlichen Gesellschaft, S.155-177



J. Cramer Verlag, Braunschweig

Ist Verkehrssicherheit berechenbar?*

PROF. DR.-ING. ECKEHARD SCHNIEDER

Verkehrssicherheit- und Automatisierungstechnik, TU Braunschweig
Langer Kamp 8, D-38106 Braunschweig

1. Einleitung

Mobilität in ihren vielfältigen Ausprägungen gehört seit eh und je zur Evolution von Natur und Zivilisation. Ohne Mobilität gibt es keine Fortentwicklung durch Austausch von Gütern und Informationen bis hin zu genetischem Material, wie andererseits ein Zuviel an Mobilität das notwendige örtliche Verweilen zu produktiven Zwecken erstickt. Jegliche menschliche Mobilität hat daher einen optimalen Grad, der in der Regel durch das so genannte Mobilitätsbudget im zeitlichen Aufwand pro Tag gemessen wird und sich mit ca. 1,5 h/Tag/Person über lange Zeit als unverändert erweist [KÜHNE].

Mobilität als physische Bewegung von Menschen und Gütern verlangt Energie zur Bewegung und speichert diese in den bewegten Objekten. Verläuft die Bewegung der mobilisierten Objekte nicht in den geplanten und vorgesehenen Bahnen, kommt es zu Kollisionen, Kontaminationen, Explosionen usw. deren Schwere insbesondere von der transportierten Menge Personen und Art der Güter sowie ihrer geschwindigkeitsabhängigen Energie abhängt. Insofern birgt Mobilität ein latentes Risiko, dessen Darstellung einerseits großes mediales Interesse findet, vor allem bei spektakulären Unfällen mit hohen Schäden, und andererseits in gesetzlichem Auftrag und zu juristischer Verfolgung nahezu lückenlos dokumentiert und in anonymisierter Form verdichtet und statistisch dokumentiert wird.

Mobilität, insbesondere mit motorisierten Verkehrsmitteln wie Automobil, Zug und Flugzeug, eröffnet neue Horizonte, die mit einem entsprechenden Risiko erkaufte werden müssen, das zum natürlichen Lebensrisiko hinzukommt. Insofern stellt sich aus ethisch-humanen Gründen die Aufgabe, zu akzeptablen Risiken im Verhältnis zu den Chancen zu kommen, welche die technischen Formen der Mobilität bieten. Allerdings darf man nicht vergessen, dass der technische Fortschritt in höchst komplexer Weise in die gesellschaftliche und natürliche Evolution integriert ist. Häufig werden diese Abhängigkeiten nicht wahrge-

* Vortrag gehalten beim Kolloquium anlässlich der Jahresversammlung der Braunschweigischen Wissenschaftlichen Gesellschaft am 07.05.2004.

nommen oder ignoriert und in ihrer Verhältnismäßigkeit der Mittel- bzw. Kosten-Nutzen-Abwägung verzerrt dargestellt oder falsch interpretiert, indem häufig an Symptomen kuriert wird, die falschen Schuldigen identifiziert werden, weil das verwickelte technisch-soziale Beziehungsgeflecht in seiner ganzen Komplexität (noch) nicht erfasst werden kann.

Hierzu ist einerseits anfänglich die phänomenologische Erfassung von Mobilität und ihren Eigenschaften erforderlich, die jedoch immer im konzeptionellen Kontext steht. Darauf können erst über eine sorgfältige Begriffsbildung die Phänomene formuliert und strukturiert werden. Erst auf dieser Basis ist eine verbindliche Beschreibung zwecks Vergleich, Bemessung und Quantifizierung möglich, jedoch alles aus der betroffenen aber passiven Außensicht. Dies wird im 2. Kapitel behandelt.

Eine detaillierte Analyse im 2. Kapitel aus der Innensicht der Systeme hinsichtlich ihrer Verlässlichkeitseigenschaften ist andererseits unerlässlich, um die Verlässlichkeit mittels Systemgestaltung an Zielgrößen auszurichten. Hier besteht die Aufgabe darin, System- und Verlässlichkeitseigenschaften begrifflich in Einklang zu bringen und über eine geeignete Modellbildung ganzheitlich zu erfassen. Mittels dieser Modelle werden verschiedene Maßnahmenkonzepte aufgezeigt und hinsichtlich ihrer Effektivität qualitativ und quantitativ berechenbar.

Die detaillierte Bestimmung vorgegebener Größen zur Verlässlichkeit für die Entwicklung sicherer und verlässlicher Systeme bezüglich ihres betrieblichen Einsatzprofils, ihrer Funktionalität, der Steuerung und Überwachung sowie ihrer technischen Realisierung mit den notwendigen Verlässlichkeitsdaten mit Hilfe eines modularen Modellierungskonzeptes wird im letzten Textkapitel vorgestellt. Mit einer Zusammenfassung und einem Ausblick schließt der Beitrag ab.

2. Phänomenologie der Verkehrssicherheit

Sicherheit und Verfügbarkeit sind Positivbegriffe wie Verlässlichkeit, Gesundheit, Wahrheit. Zur Quantifizierung dieser Begriffe wird – wohl wegen ihres idealen Charakters und seiner demzufolge unerreichbaren Vollendung – das jeweilige besser fassbare Komplement jedoch negativer Konnotation verwendet wie Schaden, Risiko, Ausfall, Fehler, Krankheit usw.

Die psychologische Wirkung der negativen Ausprägung und Bemessung an sich positiver Eigenschaften darf nicht ignoriert werden. So wird z.B. dank medialer Präsenz der Unfall an sich absolut vermittelt und macht betroffen, die Verhältnismäßigkeit bezüglich fast immer erfüllter Mission verbleibt, ist aber auch schwer vermittelbar und bislang nur wenig intuitiv qualifizierbar und quantifizierbar. Hier soll ein neuer positiver Ansatz vorgeschlagen werden.

Tabelle 1: Maße der Verlässlichkeit im Verkehr

Risiko bzgl. Unfälle (Mortalität)	<ul style="list-style-type: none"> – der Anzahl der Unfälle per Verkehrsmittelkilometer – Anzahl der Toten und Verletzten per Verkehrsmittelkilometer – Anzahl der Toten und Verletzten per Verkehrszeit
Risiko bzgl. der Beinaheunfälle (Beispiel Eisenbahn)	<ul style="list-style-type: none"> – Anzahl der Schienenbrüche, Signalfehler, usw. per Verkehrsmittelkilometer – Anzahl SPAD per Verkehrsmittelkilometer – Anzahl der Rad- und Achsbrüche im Betrieb
Risiko bzgl. der Unfallfolgen Mortalität	<ul style="list-style-type: none"> – Unfallkosten per Verkehrsmittelkilometer – Anzahl der verlorenen Arbeitsstunden der betroffenen Personen – Anzahl der Gestorbenen im Zeitraum / Anzahl der Individuen der Population im Zeitraum
Volkswirtschaftliche Kosten	<ul style="list-style-type: none"> – Staukosten – Wiederherstellungskapital – Humankapital – Zahlungsbereitschaft
LQI	– Life Quality Index
...	...Rückrufaktionen, Pannenstatistik

Parallel zur psychologischen Wahrnehmung und vielleicht auch in kausalem Zusammenhang steht die Nichtmessbarkeit positiver Werte bzw. die meist erst physikalische Messbarkeit ihrer negativen Komplemente unter Nutzung energetischer Wirkung, z.B. Schaden = Deformation, Krankheit = Fehltage, Risiko = Todesfälle usw. Hier wird bereits zur linguistischen Formulierung und der symbolischen Formulierung in Vorbereitung der späteren quantitativen Formalisierung eine erste Notation von Sicherheits- bzw. Verlässlichkeitsbedingungen angegeben. Da Verlässlichkeitseigenschaften nur in kollektiver Hinsicht quantifiziert werden, ist der Bezug auf statistische Angaben unter Verwendung von Häufigkeiten sinnvoll.

Die Begriffe der Verkehrssicherheit werden durch eine Vielzahl von Statistiken dargestellt, die unterschiedliche Größen, z.B. Verkehrsunfälle: Anzahl der Verkehrsunfälle, Anzahl der Getöteten, Menge der volkswirtschaftlichen Kosten bis hin zu hoch verdichteten Maßen wie dem LQI (Life Quality Index) ausweisen. Tabelle 1 zeigt eine Zusammenstellung von Eigenschaften und ihren Maßgrößen, Sicherheit zu qualifizieren und quantifizieren.

Das Risiko wird üblicherweise über Gefährdungshäufigkeit und Schadensausmaß definiert. Neben der Möglichkeit, das Schadensausmaß insbesondere durch

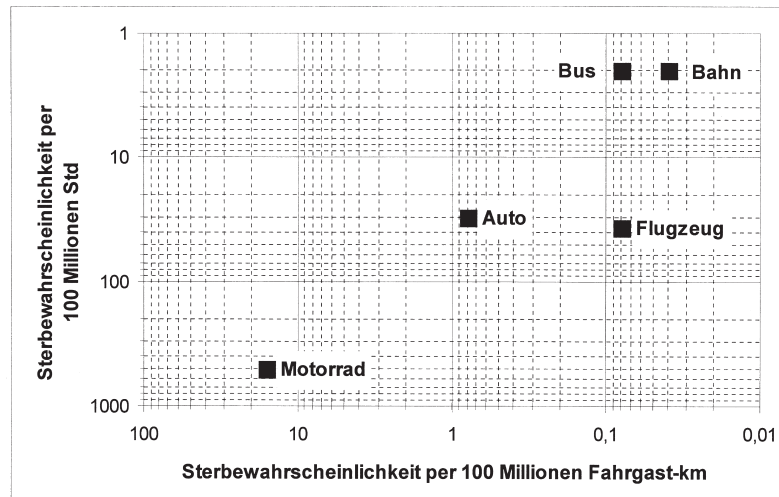


Bild 1: Risiken der Verkehrssysteme in Bezug auf Aussetzung in Reisedauer und Reiselänge (Quelle: SNCF)

eine passive Sicherheit (z.B. der Fahrzeuge, der Strecke) und durch das Rettungsmanagement zu beeinflussen, ist die Gefährdungshäufigkeit auch von technischen Systemparametern (Gefährdungsrate in $[\text{Std}^{-1}]$) des Leitsystems, Strecke und Fahrzeugen und von betrieblichen Charakteristiken des Verkehrs (Fahrzeuge pro Stunde) abhängig. Die Aussetzungsdauer spielt bei der Bewertung des individuellen Risikos eine entscheidende Rolle (Bild 1). Diese hängt von der Länge der notwendigen Reisezeit sowie von ihrer möglichen Verlängerung durch die betriebliche Unverfügbarkeit (z.B. in Stunden pro Jahr) ab. Insofern ist hier schon ein enger Zusammenhang zwischen Verfügbarkeit und Sicherheit ersichtlich. Da die genannten Einflussgrößen in zeitabhängigen Größen angegeben werden, liegt es nahe, auch für das Risiko die Zeit als entscheidenden Bezugswert zu belassen.

Interessant ist in diesem Zusammenhang auch die nationale Korrelation von Maßen der Verkehrssicherheit im Verhältnis zur jeweiligen Verkehrsstärke. Hier lässt eine erste Schlussfolgerung eine positive Korrelation von Verkehrssicherheit und Verkehrsstärke zu, die gegebenenfalls dazu Anlass gibt, dass durch größere Verkehrsdichte ein Sicherheitsgewinn erzeugt wird, möglicherweise durch zwangsläufig homogenere Verkehrsströme. Positive Entwicklungen der Verkehrssicherheit können über die letzten Jahrzehnte beobachtet werden, jedoch wird die positive Entwicklung bei den Verkehrstoten durch die kaum veränderten Unfallzahlen etwas getrübt. Hinsichtlich der altersbedingten Mortalität zeigen die Werte, dass insbesondere bei jungen Männern zwischen 15 und 20 Jahren ein erheblicher Anstieg der verkehrsbedingten Mortalität zu beobachten ist (Bild 2).

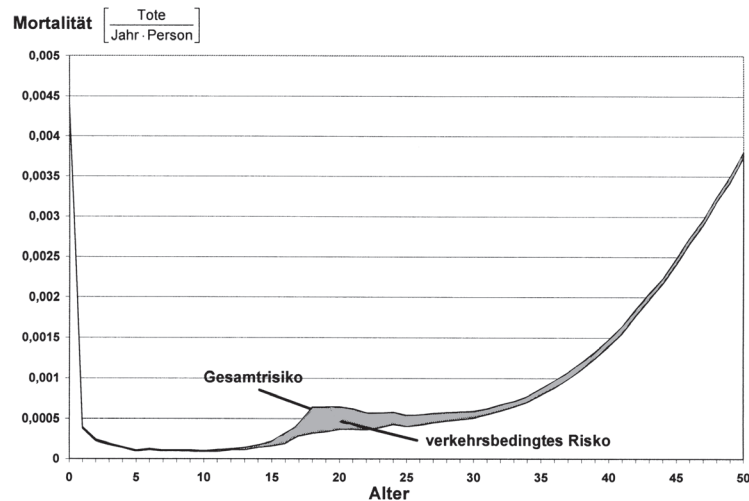


Bild 2: Mortalität durch Verkehr, Deutschland 2001(Quelle: destatis)

Primär in der retrospektiven Datenerhebung aus in der Realität beobachtbaren Werten lassen sich Aussagen zur Verkehrssicherheit herleiten. Prognosen über eine zukünftige Entwicklung der Verkehrssicherheit lassen sich jedoch nur auf der Basis von Modellen gewinnen, die durch Datenerhebung, aber auch Experimente in Versuchen und mit Simulatoren gewonnen werden.

3. Maße der Verlässlichkeit im Verkehr

3.1 Maße der Verfügbarkeit

Die betriebliche Verfügbarkeit wird einerseits durch die primäre Unverfügbarkeit des Systems beeinflusst. Hierunter fallen alle direkten Folgen (Verspätungen) des technischen sowie menschlichen Versagens innerhalb des Systems Eisenbahn. Andererseits wirken sich auf die Unverfügbarkeit viele sekundäre Gründe aus, die aus betrieblichen Charakteristiken des Verkehrs resultieren (z.B. Folgeverspätungen). Hierunter können auch unerwartete Einflüsse von anderen Systemen (Straßenverkehr) oder anderen Faktoren (Wetter, Fahrgäste,...) subsumiert werden.

In der Literatur existieren mehrere Ansätze zur Berechnung der Verfügbarkeit hinsichtlich der primären Einflüsse [ACKERMANN], [ZASTROW], [ZHU]. Dabei ist es z.B. möglich, die Verspätungszeit einer Zugfahrt zu ermitteln, die durch Ausfall einer technischen Systemeinheit verursacht wird. Für die Einbe-

ziehung der sekundären Unverfügbarkeit ist es notwendig, die statistischen Daten über Zugverspätungen zu analysieren und zu evaluieren. Neben der Zeit, als risikorelevanter Bezugsgröße, wird als ein Gütemaß für die Verfügbarkeit sehr oft die monetäre Bewertung benutzt, insbesondere im Rahmen einer Kosten-Nutzen-Analyse.

Sei t_R die Zeit, die der mittleren idealen Reisedauer entspricht. Diese ergibt sich durch Annahme des kürzesten Weges, maximal zulässiger Wegegeschwindigkeit, maximaler Fahrzeugbeschleunigung usw. Die mittlere Verlängerung dieser idealen Reisezeit Δt ist von der Wirkung der genannten primären und sekundären Verfügbarkeitseinflüsse geprägt (Haltezeit, Haltezahl, Stauzahl, Stillstand durch Stau, technische Störung, Wartezeit, Umsteigezeit, usw.) Die Verkehrsverfügbarkeit kann dann wie folgt definiert werden:

$$A_T = \frac{t_R}{t_R + \Delta t_R} \quad , \quad A_T \in [0,1], \mathbb{R} \quad (1)$$

Als Komplement kann die Verkehrs-Unverfügbarkeit als

$$Q_T = 1 - A_T \quad (2)$$

ausgedrückt werden. Die Vergleichbarkeit der Verfügbarkeit unterschiedlicher Verkehrssysteme kann mittels der Definition eines Verkehrsverfügbarkeitspotenzials pA_T erreicht werden:

$$pA_T = -\lg Q_T = -\lg \frac{\Delta t_R}{t_R + \Delta t_R} \quad , \quad pA_T \in [0,\infty), \mathbb{R} \quad (3)$$

Für $\Delta t_R \ll t_R$ kann die Berechnung vereinfacht werden:

$$pA_T = -\lg \frac{\Delta t_R}{t_R} \quad (4)$$

3.2 Maße der Sicherheit

Als Größe für die Bewertung des individuellen Risikos wird häufig die Anzahl der Toten pro Person und Jahr empfohlen, wobei die Risikoakzeptanz z.B. auf dem Vergleich mit der minimalen endogenen Mortalität basiert oder durch Vergleich auf bestehenden Statistiken beruht.

Das aus der Benutzung eines Systems resultierende Risiko für ein Individuum hängt stark von der kumulierten Gesamtzeit der Aussetzung ab und ist folglich

proportional zu der menschlichen Lebensdauer. Diese beträgt in Deutschland in 2003 durchschnittlich 78,09 Jahre (Männer 75,11 Jahre, Frauen 81,07 Jahre), was einer durchschnittlichen Mortalität (als Kehrwert der mittleren Lebensdauer) $1/78,09 = 0,0128$ pro Jahr entspricht. Unter der Annahme minimaler menschlicher Sterblichkeit, der so genannten minimalen endogenen Mortalität mit $2E-4$ Tote pro Jahr/Person, erhält man eine maximale Lebenserwartung von 5.000 Jahren, was die Risikobewertung nicht mehr intuitiv verständlich macht.

Ein alternativer Ansatz ist die Betrachtung des Risikos als potenzielle Verkürzung des menschlichen Lebens [HEILMANN]. Dieses Risikomaß wird häufig in der Medizin verwendet, insbesondere für die Veranschaulichung der negativen Folgen von gesundheitsschädlichen Angewohnheiten (z.B. Rauchen), aber auch von körperlichen Aktivitäten (bestimmte Sportarten, Berufe).

Die Verkürzung des menschlichen Lebens durch ein Verkehrssystem ΔT_{HT} kann wie folgt definiert werden:

$$\Delta T_{HT} = T_H - T_{HT} \quad (5)$$

wobei die T_H der mittleren menschlichen Lebensdauer ohne den Einfluss des Verkehrssystems entspricht und T_{HT} die mittlere menschliche Lebensdauer mit Benutzung des Verkehrssystems darstellt. Der Wert T_H kann aus den altersabhängigen Statistiken über die Lebensdauer und Unfall-/Tötungshäufigkeiten bestimmter Zielgruppe der Personen ermittelt werden.

Aus der Beziehung

$$T_H = \int_0^{\infty} e^{-\int_0^t M_H(\tau) d\tau} dt = \frac{1}{M_{HM}} \quad (6)$$

kann der Wert der mittleren menschlicher Mortalität M_{HM} ohne den Einfluss des Verkehrssystems abgeleitet werden. Ähnlich gilt für die T_{HT} :

$$T_{HT} = \int_0^{\infty} e^{-\int_0^t (M_H(\tau) + M_T(\tau)) d\tau} dt = \int_0^{\infty} \left(e^{-\int_0^t M_H(\tau) d\tau} \right) \left(e^{-\int_0^t M_T(\tau) d\tau} \right) dt = \frac{1}{M_{HM} + M_{TM}} \quad (7)$$

wobei M_{TM} die mittlere durch den Verkehr verursachte Mortalität darstellt. Neben der Ermittlung der M_{TM} aus den Unfallstatistiken ist es möglich, die Mortalitätsrate eines Verkehrssystems (bzw. seines Teilsystems) im Rahmen einer Risikoanalyse zu berechnen (z.B. nach [SLOVAK03]).

Mit diesem Ansatz kann der Risikobeitrag eines konkreten Teilsystems in Form der Verkürzung der menschlichen Lebensdauer dargestellt werden. Eine Ent-

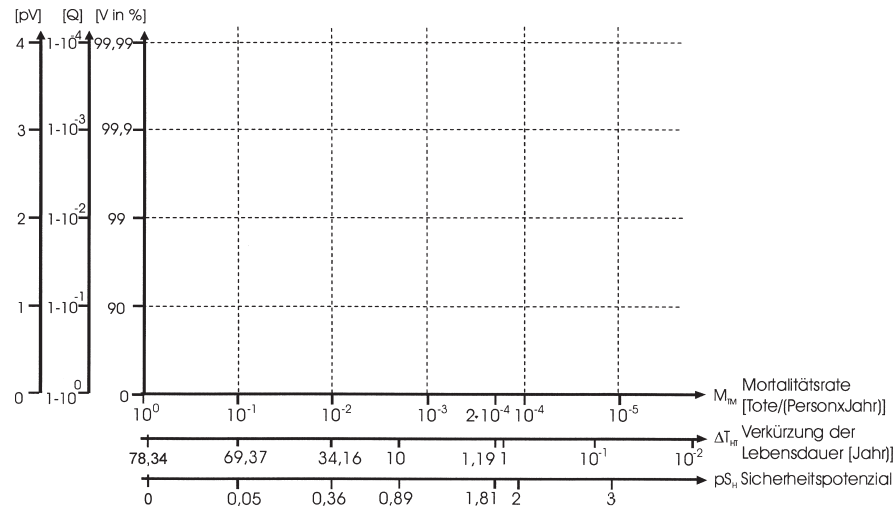


Bild 3: Quantitative Skalierung des Sicherheits- und Verfügbarkeits-Diagramms

scheidung über die Risikoakzeptanz kann erst unter Berücksichtigung der Beiträge anderer Teilsysteme bzw. deren mehrmalige Benutzung getroffen werden. Aus diesem Grund ist es sinnvoll, den Einzelbeitrag eines Teilsystems auch in Form des menschlichen Sicherheitspotenzials darzustellen:

$$pS_H = -\lg \frac{M_{TM}}{M_{HM} + M_{TM}} \quad (8)$$

bzw. unter der Annahme: $M_{HM} \gg M_{TM}$:

$$pS_H = -\lg \frac{M_{TM}}{M_{HM}} \quad (9)$$

Eine Umrechnung auf die Verkürzung der menschlichen Lebensdauer ist jederzeit unter der Kenntnis der T_H möglich.

$$pS_H = -\lg \frac{\Delta T}{T_H} \quad (10)$$

Die Verkürzung menschlicher Lebensdauer sowie das Sicherheitspotenzial können dem Verfügbarkeitspotenzial nach Kap. 3.1 gegenübergestellt werden. Das Bild 3 zeigt das dadurch gewonnene Koordinatensystem mit der logarithmischen Verfügbarkeits- und Sicherheitsskala nach [SCHNIEDER03].

4. Formalisierung der Verlässlichkeit

4.1 Verlässlichkeitsbezogene Aspekte der Verkehrssicherheit

Eine Differenzierung verschiedener Systembetriebszustände mit vollständig fehlerfreiem Betrieb, eingeschränktem Betrieb, gefährlichem Betrieb, sicherem Zustand, eingetretenem Schadensfall und Rettung bzw. Instandsetzung außerhalb des operativen Betriebes usw. zeigt Bild 4 mit den vier korrespondierenden Quadranten der Verlässlichkeit im so genannten Sicherheits-Verfügbarkeits-Diagramm von Bild 3.

4.2 Formalisierung der Sicherheit im physikalischen Zustandsraum

Sicherheit als subjektiv empfundene Eigenschaft drückt sich im Verkehr häufig komplementär als Vermeidung von Gefahren, Schäden und Verlusten der an Transportprozessen beteiligten Personen und Sachen aus. Damit kann die Wirkung der Verkehrssicherheit ausschließlich in Bezug zu physischen Ausprägungen gesetzt werden.

Eine abstrakte formale Beschreibung der Schäden kann einfach erfolgen, indem der schadensfreie Zustand als Ideal postuliert wird bzw. Grenzwerte physika-

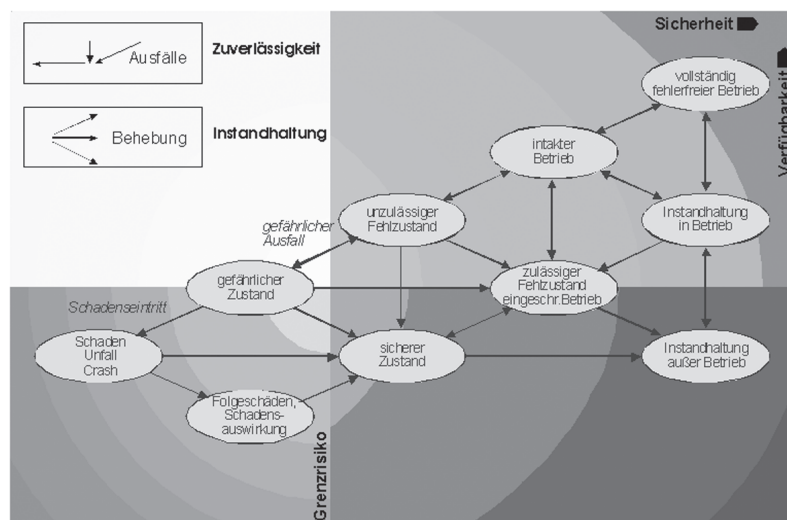


Bild 4: Differenzierung verschiedener Systembetriebszustände in der Verfügbarkeits-Sicherheitsebene

lisch-chemischer Natur angegeben werden, die einzuhalten sind. Der schadensfreie Zustand x_{safe} ist primär auf ein Bezugsobjekt bezogener Zustand $x_{\text{safe,object}}$, aus dem insgesamt auf einen sicherheitsbezogenen Zustandsraum $X_{\text{safe, bound}}$ geschlossen werden kann, der allerdings mehrere Bezugsobjekte einbezieht, z.B. ein oder mehrere Fahrzeuge.

Ein Beispiel für die sicherheitskritische Bewegung im Zustandsraum ist das Verlassen der Fahrbahn von Fahrzeugen, z.B. infolge überhöhter Geschwindigkeit oder bei Seitenwind oder Glatteis. Für die sicherheitsrelevante Bewegung von Transportmitteln sind grundsätzlich die vier Teilzustandsräume „Stillstand (A)“, „sichere Bewegung (B)“, „gefährliche Bewegung (C)“ und „Schaden (D)“ zu unterscheiden (Bild 5b):

Zu beachten ist, dass einem Schadenseintritt eine system- und bewegungsbedingte kausale Zustandsfolge vorausgeht, die als Trajektorie im (vollständigen) Zustandsraum abgebildet werden kann. In der Regel ist der Übergang vom sicheren in den gefährlichen Zustand und dann zum Schaden unmittelbar und zwangsläufig und irreversibel. Daher muss bereits die kausal ursächlichste und initiale Verletzung des erlaubten Zustandsraumes verhindert werden.

Der erlaubte Zustandsraum ergibt sich dabei aus dem Minimum zwischen den aktuell zulässigen Grenzwerten, -flächen und der Eigendynamik der Fahrzeugbewegung unter Berücksichtigung dieser Grenzwerte, die ihrerseits auch zeitlichen Änderungen unterliegen.

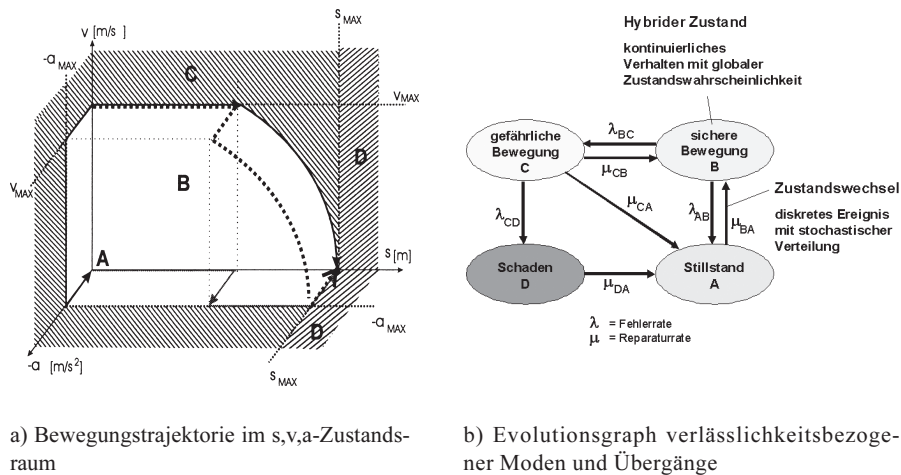
4.3 Modellierung der Bewegungstrajektorie

Die Trajektorie kontinuierlicher Bewegung eines Fahrzeuges auf linearer Strecke bis zum gefahrlosen Halt, z.B. vor einer Kreuzung, Weiche oder Kurve, auf den Grenzflächen des erlaubten Zustandsraums mit den Koordinaten Beschleunigung, Geschwindigkeit und Weg zeigt Bild 5a.

Der Durchtritt einer aus der Fahrzeug-Eigendynamik und aus richtiger oder fehlerhaft wirkender Regelung resultierenden Trajektorie durch die Grenzflächen des sicheren Zustandsraumes kann als diskretes Ereignis aufgefasst werden. Insofern kann das komplette Systemverhalten vereinfacht durch den Evolutionsgraphen eines hybriden, d.h. kontinuierlich diskreten Systems mit vier Zustandsmoden beschrieben werden (Bild 5b) [ENGELL].

4.4 Modellierung der Verkehrssicherheit im multihybriden Zustandsraum

Die einzelnen Betriebszustände werden neben den kontinuierlichen Zuständen des physikalischen Modells innerhalb der Moden zusätzlich durch zuverlässig-



keitstechnisch diskrete und zeitlich stochastische Übergänge (events) und wahr-scheinlichkeitsstheoretisch attributierte diskrete Systembetriebszustände unterschieden (vgl. Bilder 5a und b). Dies ist beispielsweise der intakte oder defekte Betriebszustand eines Sensors, Aktors oder einer Steuerung.

In gleicher Weise können jedoch „menschliche Funktionsträger“ in die Modellierung einbezogen werden, wenn ihr Verhalten hinsichtlich der Abweichungen von der idealen Trajektorie einer sicheren Verkehrs- bzw. Fahrzeugsteuerung in Form probabilistischen Ausfallverhaltens stochastisch modelliert wird.

Die diskreten verlässlichkeitsbezogenen Betriebszustände bzw. -übergänge sind in der Regel nur statistisch beschreibbar, d.h. durch Zustandswahrscheinlichkeit und -übergangsraten, die zudem situationsabhängig variieren. Damit wird das hybride Modell diskret-kontinuierlicher Verhaltensdynamik noch um die stochastische Verlässlichkeitsdynamik ergänzt und wahrscheinlichkeitstheoretisch attribuiert. Diese zweifach hybride Modellierung im erweiterten Zustandsraum (physikalische Zustände, informationelle Betriebszustände) konzentriert somit die verschiedenen Sichten in einer einzigen Darstellung mit Mengen mathematischer Attributierung, kontinuierlichen Zustandsmoden und Wahrscheinlichkeiten sowie diskreten Übergangsflächen.

5. Maßnahmen zur Sicherheitsgewährung

Dieser Modellierungsansatz lässt sich nun auch zur methodischen Separation in abstrakt-funktionaler und konkret-realisierungsbedingter Hinsicht nutzen.

- a) Die analytische Forderung kann funktional durch regelungstechnische Aufgaben gelöst werden. In funktionaler Hinsicht lässt sich die Sicherheit unmittelbar auf eine regelungstechnische Betrachtung überführen und die Aufgabe zur Sicherheitserzielung als Einhaltung eines begrenzten Zustandsraumes formulieren. Der erlaubte Zustandsraum wird allgemein durch Hyperflächen aufgespannt, welche aus den zulässigen Grenzwerten, der systeminternen Dynamik vorzugsweise der Transportmittel sowie aktuellen Systemgegebenheiten (z.B. Fahrerlaubnis, Grünsignalisierung, Umgebungsbedingungen, andere Verkehrsteilnehmer, Zustands- und Ortungsinformationen usw.) resultieren.
- b) Die verlässliche Realisierung der Aufgaben kann durch geeignete Einrichtungen automatisch bzw. durch qualifiziertes Personal manuell erfüllt werden. Die Einhaltung des erlaubten Zustandsraums muss auch in der Realität dauerhaft gewährt sein. Diese physische Sicht verlangt die zeitlich statistische Einhaltung unter Gesichtspunkten der Verlässlichkeit der Realisierung der Funktionen zur Sicherheitsgewährung.

Schwierig ist dabei

- die Konkretisierung des Zustands in Form physikalischer Größen (Zustandsvektor bzw. -übergangsfunktion)
- eine aktuelle Bestimmung der Verkehrssicherheitsgrenze infolge dynamisch veränderlicher Situationen
- die objektive Bewertung des Zusammenhangs zwischen individuellen Grenzübertretungen und kollektivem Sicherheitsempfinden, weil dieses nicht statistisch wahrgenommen, sondern häufig und medial verstärkt wird
- die Ermittlung des (gewichteten) Zusammenhangs zwischen den physikalischen Größen (Zustand) und dem Risiko, insbesondere dem Schaden, der in der Regel durch Tote, Verletzte unterschiedlicher Schwere bzw. Verlust oder Beschädigung von Gütern, Transporteinrichtungen sowie der Umwelt gemessen wird. Der Zusammenhang kann über abgeleitete Zustandsgrößen vor dem propagierten Schadenseintritt, d.h. an der Zustandsraumgrenze hergestellt werden.

Das ethisch bedingte Ziel, die Verkehrssicherheit zu steigern, verlangt nach geeigneten Maßnahmen wie dies zu erreichen ist. Die (probabilistische) Einhaltung des zulässigen Zustandsraumes bei Transportprozessen kann nun durch unterschiedliche Prinzipien erreicht werden. Sie können in methodische, betriebliche, funktionale und technische Aspekte eingeteilt werden, die z. T. überlappen.

Zu methodischen Aspekten gehören die Regularien gesellschaftlicher, rechtlicher (gesetzlicher) und institutioneller Art, z.B. Auflagen zur sicheren Produktgestaltung, zur Schadensverhinderung bis hin zu finanziellen und persönlichen Sanktionen bei

Missachtung, Fahrlässigkeit, Sabotage usw., aber auch die Regularien zur sorgfältigen sicherheitsgerichteten Entwicklung, Nachweisführung, Zulassung und Betrieb mit qualifizierten Techniken, Personal und Einrichtungen.

Es lassen sich drei prinzipielle Hauptformen in der tatsächlichen Realisierung und aktuellem Betrieb finden, die sich durch die technische oder menschliche Ausübung der Bewegungssteuerung bzw. -sicherung und Funktionsstrukturen unterscheiden:

- rein menschlich verantwortete Bewegungssteuerung nach Regularien (Gesetze, Verordnungen)
- technisch assistierte und menschlich verantwortete Bewegungssteuerung
- technisch verantwortete Bewegungssicherung

Das Verlässlichkeitsverhalten der Steuerungseinrichtungen bei internen und externen Störungen, Ausfällen und Fehlern muss näher aus Sicht der Verlässlichkeit betrachtet werden.

Grundsätzlich stehen dafür mehrere Ansätze zur Verfügung, die sich in ihrer Wirksamkeit und Realisierung sowie Akzeptanz und Durchsetzungsfähigkeit unterscheiden. Hinsichtlich Wirksamkeit und Realisierung der Maßnahmen kann die Diskussion auf die Variation/Modellierung der Übergangsraten zwischen den vier grundsätzlichen Betriebszuständen fokussiert werden.

- a) Verringerung der Übergänge in den gefährlichen Betrieb (λ_{BC} , vgl. Bild 5b) z.B. durch
 - besseres menschliches Fahrverhalten (Ausbildung, Einsicht)
 - strengere Regularien (Geschwindigkeitsvorgabe) und Kontrolle: prädiktive Regelung
 - automatisiertes Fahrverhalten
 - o Tempomat
 - o Spurhaltung
 - Verkehrsleitsystem und automatische Verkehrsbeeinflussung
- b) Erhöhung der Übergangsrate zum Verlassen des gefährlichen Betriebes (μ_{BC} , μ_{CA} vgl. Bild 5b) z.B. durch
 - Fahrerassistenz
 - o Automatic Lane Departure Warning
 - o Adaptive Cruise Control
 - o Höchstgeschwindigkeitsüberwachung
 - o ABS
 - o ESP
 - o Notbremsung
 - Fahrerschulung (Sicherheitstraining)

- c) Verringerung der Unfallschwere durch so genannte passive Sicherheitssysteme (λ_{CD} vgl. Bild 5b) wie z.B.
 - Sicherheitsgurt
 - Knautschzone
 - Kopfstützen
 - Airbag
- d) Verbesserung der Rettungsmaßnahmen (μ_{DA} vgl. Bild 5b), insbesondere der Dauer von Unfalleintritt bis zur ärztlichen Hilfe.

Die Vermutung liegt nahe, die Verkehrssicherheit durch verstärkten Einsatz von Sicherheitssystemen nach anfänglich c), d) und nunmehr b) erhöhen zu können. Dies ist in den letzten Jahrzehnten mit erheblichem Erfolg geschehen, jedoch ist die Unfallhäufigkeit als solche nicht in dem Maße wie die Unfallschäden, insbesondere Unfalltote, gesunken. Mit jedem Unfall geht aber auch die Verringerung der Verkehrsverfügbarkeit einher, was sich durch die Stauhäufigkeit und Fahrzeitverlängerung ausdrückt, woraus wieder eine Verlängerung der sicherheitsrelevanten Expositionsdauer resultiert. Ein anderer indirekter Ansatz setzt bei der Maßnahme a) an, die primär die Verkehrsflüssigkeit verbessert und u.a. die Verweildauer verringert. So zeigt die Einrichtung von Verkehrsleitzentralen sowie Verkehrsbeeinflussungsanlagen mit ihren guten Wirkungen auf die Verkehrsflüssigkeit und damit Verkehrsverfügbarkeit korrespondierend auch eine Verbesserung der Sicherheit, wie aus Statistiken der jeweiligen Bereiche hervorgeht. In gleicher Weise wird durch fahrzeugbezogene Maßnahmen zur Intensivierung sicheren Betriebsverhaltens mit einer primären Erhöhung der Verkehrsflüssigkeit als Sekundäreffekt die Verkehrssicherheit erhöht.

Bild 6 zeigt im Verfügbarkeits-Sicherheits-Diagramm die Wirkung dieser unterschiedlichen Maßnahmen durch Variation der o. g. Parameter, die aus der Berechnung der Markov-Ketten aus Bild 5b ermittelt wurden. Die Gültigkeit der obigen Vermutungen wird mit dem Modell bestätigt. Das Modell muss jedoch zur Entfaltung der vollen Aussagekraft noch weiter verfeinert und hinsichtlich seiner Parameter noch weiter identifiziert und kalibriert werden.

Zusammenfassend kann jedoch konstatiert werden, dass Verkehrssicherheit und -verfügbarkeit zwei Ausprägungen der Verlässlichkeit als die Eigenschaften des Verkehrs sind. Mit Hilfe der in Zukunft möglichen Maßnahmen ist nicht nur eine Erhöhung der Verkehrsflüssigkeit und -dichte, sondern auch indirekt ein nennenswerter Beitrag zur Verkehrssicherheit möglich, der bei alleiniger Konzentration auf die Verkehrssicherheit nicht erreicht werden kann.

Ist Verkehrssicherheit berechenbar?

169

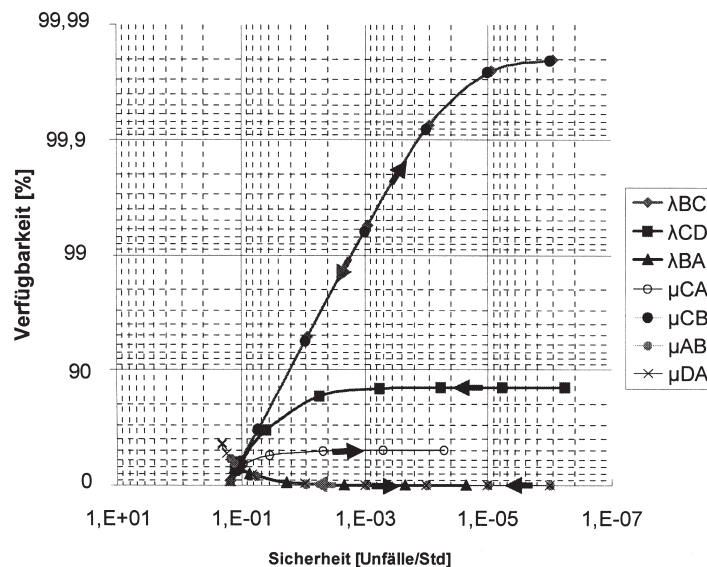


Bild 6: Verfügbarkeits-Sicherheits-Diagramm, Variation der Parameter von Fehler- und Reparaturraten

6. Beitrag der Automatisierungstechnik

Die grundsätzlichen Aufgaben einer sicheren Bewegung im zulässigen Zustandsraum werden durch ein geeignetes Zusammenspiel folgender elementarer Funktionen in der Funktionsstruktur eines Regelkreises nach Bild 7 bewältigt.

- A Ermittlung der Führungstrajektorien nach Maßgabe der Transportaufgabe und Verkehrssituation
- B Begrenzung der Führungstrajektorien ggf. nach Maßgabe des Verkehrsweges und der Verkehrssituation
- C Ermittlung des aktuellen Verkehrszustands (-vektors/-trajektorie)
- D Regelung bzw. Steuerung und Vorgabe des Stellgrößen- und Ausführungsvektors/trajektorie mit Begrenzung der Stellgrößen.

Varianten dieser Grundstruktur ergeben sich durch Ausprägung der Regelungsstruktur, Systemdynamik der Regelung, Anordnung der Funktionseinheiten (Allokation) zentral und/oder fahrwegseitig bzw. mobil verkehrsmittelseitig und insbesondere die Ausführung der Funktionen inkl. Signalisierung/Kommunikation durch

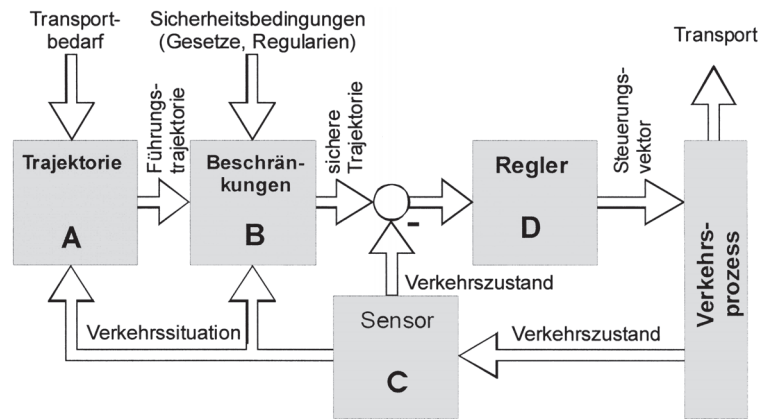


Bild 7: Grundlegende Regelkreisstruktur für Sicherheitsaufgaben

- technische Funktionsträger - entweder passiv, d.h. konstruktiv-materiell, oder aktiv, d.h. als regelungstechnisch-energetisch,
- menschliche Funktionsträger, oder in
- Kombination technisch-menschlicher Funktionsträger.

Die „großen“ Probleme der sicherheitsrelevanten Regelung im Verkehr resultieren aus der Komplexität infolge Kombinatorik der Aspekte und lassen sich folgendermaßen artikulieren:

richtige zeitgerechte Ermittlung

- der richtigen verkehrssituationsbezogenen Führungstrajektorie (A)
- des zulässigen Zustandsraumes (B)
- des tatsächlichen Verkehrszustands (C).

Die richtige Ermittlung richtiger Größen bezieht sich dabei auf Korrektheit, Aktualität, Genauigkeit, Präzision und Auflösung, d.h. insgesamt auf informationsbezogene und messtechnische Merkmale, zu denen die richtige Entwicklung sowie geeignete Verkehrsformen hinzukommen, welche durch die vorgelagerten normativen Rahmenbedingungen determiniert sind.

6.1 Grundsatzfragen verlässlicher Systeme

Grundsätzlich ist bei Ausführung notwendiger oder auch nur gewünschter Funktionen zur sicheren Fahrzeugführung der Zweck einer Automatisierung abzuwägen. Der Zweck bezieht sich zwar vordergründig auf die Alternativen der Aus-

führung entweder durch den menschlichen Bediener oder durch den geräte-technischen Automat, muss aber auch auf den Zweck der Funktion selbst bezogen werden, wodurch sich eine neue wechselseitige Beziehung zwischen Funktion und Ausführung ergibt, die neben der einseitigen Richtung Zweck-Funktion-Ausführung auch die entgegen gesetzte (reflexive) Relation Ausführung-Funktion-Zweck umfasst.

Neben klassischen Sicherheitsbetrachtung implementierungsspezifischer Verlässlichkeit vor allem im operativen Einsatz (RAMS) tritt durch diese Sicht eine neue Dimension: Die Korrektheit der implementierungsunabhängigen Funktion, die im Wesentlichen von der Komplexität der Funktion selbst abhängig ist und vor allem eine Frage der Funktionsspezifikation und ihrer algorithmisch programmtechnischen Formalisierung ist. Stillschweigend akzeptiert wird, dass hoch komplexe Funktionen kaum vollständig korrekt sind.

Unter Korrektheit wird verstanden, dass jede mögliche Zustands- bzw. Wertekombination zu einer erwartungsgemäßen Folgekombination führt. Beispiele der Inkorrektheit sind Überläufe von Zahlen oder Speichern, undefinierbare Anfangszustände oder Speicheradressen usw., aber auch fehlende Handlungsaktionen oder unvollständige Situationsdarstellungen.

Zwangsläufige Konsequenz der bei zu großer Komplexität unkorrekten Arbeitsweise ist sowohl bei menschlichen als auch (vom Menschen entworfenen) technischen Systemen die Nichterfüllung von Funktionen und damit eine Beeinträchtigung der Sicherheit.

Konsequent kann folgender Zusammenhang qualitativ vermutet werden:

- hoch zuverlässige Systeme sind nicht komplex (Beispiel Transistoren, Zellen, Kristalle)
- hoch komplexe Systeme sind nicht zuverlässig (Beispiel Betriebssysteme, Menschen, Gesellschaften).

Insofern kann man zur Sicherheitserzielung bei menschlich verantworteter Führung – da sich die menschliche Korrektheit bzw. Zuverlässigkeit nicht bzw. nur begrenzt steigern lässt – die Funktions- bzw. Aufgabenkomplexität reduzieren (Beispiel: Restriktion der Höchstgeschwindigkeit, Kreuzungsfreier Betrieb, nur Rechtsabbiegen, Spurwechsel-/Überholverbot, Gegenspurtrennung usw.) oder bzw. und die Korrektheit technischer Systeme ausreichend steigern. Da bei Menschen sowohl die inhaltlich korrekte Funktion als auch die zeitlich zuverlässige Funktion nicht signifikant verbesserbar sind, scheint die automatische Funktionsausübung mit hoch zuverlässiger Technik bei gleichzeitiger Steigerung der Korrektheit wie Verringerung der Aufgabenkomplexität eher Erfolg versprechend.

6.2 Realisierungsvarianten sicheren Betriebes

Für das Implementierungsziel Verlässlichkeit lassen sich grundsätzlich zwei Extremvarianten finden:

- komplett automatische hoch zuverlässige Funktionsausführung (und menschliche Überwachung der richtigen Wirkung)
- menschliche Funktionsausführung mit automatischer Überwachung (und zusätzlicher Überwachung der automatischen Überwachung zur Erzielung höchster Zuverlässigkeit).

In beiden Varianten wird die Verkehrskomplexität primär mit der automatischen Funktionsausführung beherrscht und profitiert sowohl von einer Absenkung der verkehrlichen Komplexität (vgl. automatische Bahnen mit reduzierter betrieblicher Komplexität und restriktiven Zugängen) als auch von einer gesteigerten Korrektheit der Funktionsspezifikation und ihrer Formalisierung in Algorithmen und Programmen.

In der tatsächlichen Realisierung lassen sich drei prinzipielle Hauptformen finden, die sich durch die technische oder menschliche Ausübung der Bewegungssteuerung bzw. -sicherung und Funktionsstrukturen unterscheiden:

- (1) rein menschlich verantwortete Bewegungssteuerung
- (2) technisch assistierte menschlich verantwortete Bewegungssteuerung
- (3) technisch verantwortete Bewegungssicherung.

Aus sicherheitstechnischer Sicht muss nun insbesondere das Verlässlichkeitsverhalten der Steuerungseinrichtungen bei internen und externen Störungen, Ausfällen und Fehlern betrachtet werden.

Eine erste einfache Analyse muss die Verlässlichkeit der einzelnen automatisierungstechnischen und menschlichen Teilsysteme modellieren, was insbesondere den Kontext zur jeweiligen Aufgabe berücksichtigen muss, wobei jedoch das menschliche Fehlverhalten in der Regel im aktuellen Verkehrsgeschehen gegenüber dem technische Fehlverhalten dominiert. Setzt man für die sicherheitsrelevante Verfügbarkeit der Teilsysteme an $V_{H(uman)}$, $V_{A(ssist)}$, $V_{V(ehicle)}$, so ist aufgrund der Serienstruktur für die Zuverlässigkeit der Assistenz wegen $V_A, V_V \sim 1$ und somit der menschliche Faktor weitestgehend entscheidend, der allerdings infolge der Warn-Assistenzfunktionen verbessert wird. Erst bei einer parallelen Assistenz mit Eingriffsberechtigung im kritischen Fall wird die sicherheitsrelevante Verfügbarkeit gesteigert werden.

$$V_{System} = (V_H + V_A - V_H \cdot V_A) \cdot V_V > V_H V_V \quad (11)$$

Was in diesem Fall sehr einfach formuliert wird, ist bei detaillierter Analyse höchst kompliziert, da im Assistenzsystem viele komplexe Einzelfunktionen technisch einwandfrei arbeiten müssen, die in der Regelkreis-Verknüpfung wieder eine zuverlässigkeitstechnische Serienstruktur aufweisen.

Auf die wichtige Frage der Migration bzw. Übertragung von menschlicher Beherrschung von komplexen Situationen zur automatischen Fahrzeugführung kann hier nicht eingegangen werden. Dies verlangt die Erstellung korrekter Funktionen und verlagert die Sicherheit in den vorgelagerten Entwurfs-, Entwicklungs- und Produktionsprozess. Auch hier gilt der gleiche Zusammenhang zwischen Komplexität und Verlässlichkeit menschlicher und technisch gestützter Entwicklung, die heute mit geeigneten Werkzeugen vorgenommen wird. Unter Verweis auf die Arbeiten zur Entwurfsautomatisierung [SCHNIEDER99], [BIKKER] kann insbesondere nach dem Methodenrahmen BASYSNET ein weitestgehend durchgängig werkzeuggestützter Entwicklungsprozess praktiziert werden, der eine modellbasierte, methodisch verifizierte und automatisierte Entwicklung ermöglicht. Diese moderne Art der Softwareproduktion, die verbleibende Fehlerursachen durch Tests ebenfalls auf Modellbasis identifiziert, ermöglicht bereits hoch korrekte Funktionen.

Mit der ergänzenden Modellierung der menschlichen und technischen Ressourcen nach der PROFUND-Methode können sowohl quantitative Verfügbarkeit als auch Sicherheitsziele normkonform ([IEC 61508], CENELEC [EN50126]) skaliert und die technischen Einrichtungen parametrisiert werden [SLOVAK03].

Eine grundsätzliche, bis heute ungelöste Problematik informationsverarbeitender Einrichtungen zur Sicherheitsverantwortung ist die Aufteilung auf Programme und Gerätetechnik. Wegen der grundsätzlichen Fehleranfälligkeit beider Anteile wurden so genannte diversitäre oder dissimiläre Ansätze verfolgt, jedoch dominiert die Zahl der Ansätze mit Hardwarefehler toleranz und einfachkanaliger, jedoch korrekter programmierter Funktionalität. Diese Philosophie entspricht auch der grundsätzlichen Struktur des vorliegenden Beitrags, in dem die Funktionalität der Sicherung als solche formal modelliert und somit beweisbar wird.

Diesen Zusammenhang unterstreichen auch die von europäischen Normen [EN 50128] begleiteten großen Anstrengungen beim Einsatz formaler Techniken, d.h. Beschreibungsmittel und Methoden auf mathematisch fundierter Basis, um mit geeigneten rechnergestützten Werkzeugen die Funktionalität der Sicherungseinrichtungen in Form von algorithmisierten Spezifikationen zu modellieren und ihre Korrektheit, Vollständigkeit und Widerspruchsfreiheit zu beweisen [FORMS], [FME]. Die Spezifikationen können anschließend mit Hilfe von Codegeneratoren in den Zielcode umgesetzt und implementiert werden. Eine nachfolgende Validation durch umfangreiche Tests qualifiziert die erfolgreiche und sichere technische Realisierung.

Die Verlässlichkeit der elektronischen Hardwarekomponenten aus der Massenfertigung hat dank einer hervorragenden Qualitätssicherung außerordentlich hohe Werte erreicht. Unter diesen Voraussetzungen konnten sich für sicherheitsrelevante Steuerungen besonders im Eisenbahn- und Luftverkehr sowohl für stationäre als auch mobile Einheiten Standardstrukturen etablieren, die auf Majoritätsredundanz beruhen. Hier profitieren vor allem ereignisdiskrete Sicherungsverfahren, z.B. Blocksicherung bei Zügen oder dreibegriffige/mehrbegriffige Lichtsignalanlagen bei Straßenkreuzungen oder Bahnübergängen. Bei der Überwachung und Erfassung kontinuierlicher Größen, z.B. Geschwindigkeiten, Positionen oder Hinderniserkennung wie etwa durch Multi-sensorsysteme, sind noch keine abschließenden Softwareverfahren oder Hardwarestrukturen erkennbar, wenngleich auch hier fehlertolerante Strukturen mit Selbstüberwachung und adaptierten Vertrauensintervallen im Vordergrund stehen. Dynamisch rekonfigurierbare Steuerungen für diese Aufgaben sind noch Gegenstand der Forschung, wenngleich diese Strukturen große Potentiale hinsichtlich der Verlässlichkeit aufweisen [BITSCH].

Interessant aus Sicht der Verlässlichkeit von Verkehrssystemen ist die Allokation der Steuerungsfunktion entweder zu (vielen) mobilen Einrichtungen, d.h. den Transportmitteln, oder zur Verkehrswegeinfrastruktur, wo insbesondere das Konzept zur Koordination beschränkter Fahrwegeressourcen eine stationäre Allokation gemäß offener Steuerung nahe legt. In den verschiedenen Verkehrsbereichen haben sich dem entsprechend unterschiedliche Sicherungsprinzipien und -techniken entwickelt, wie Bild 8 zeigt, was auch mit unterschiedlichen Maßen der Verlässlichkeit korreliert.

Die physische Ausführung dieser Funktionsprinzipien erfolgt entweder durch Menschen, die durch technische Einrichtungen, z.B. einfache Sensoren, aber auch komplexe Assistenzsysteme unterstützt werden oder ausschließlich durch Automatisierungsgeräte, z.B. Autopiloten, automatische Sicherungs- und Fahreinrichtungen sowohl mobil als auch stationär wahrgenommen werden [WILTSCHEK].

Die Steuerungsfunktionen brauchen jedoch dank heutiger Kommunikationstechnologien zukünftig nicht zwangsläufig ausschließlich wegeseitig angesiedelt zu werden. Offensichtlich besteht ein klares Defizit in der Kooperation strecken- und fahrzeugseitiger aktiver Regelungssysteme.

7. Zusammenfassung und Ausblick

Die formalisierte Darstellung der Verkehrssicherheit in diesem Beitrag regt die Frage nach dem möglichen quantifizierbaren Sicherheitspotenzial an. Die dafür notwendigen Daten müssen hinsichtlich des individuellen Verkehrsmodus und dem jeweiligen Automatisierungsgrad einzeln ermittelt werden.

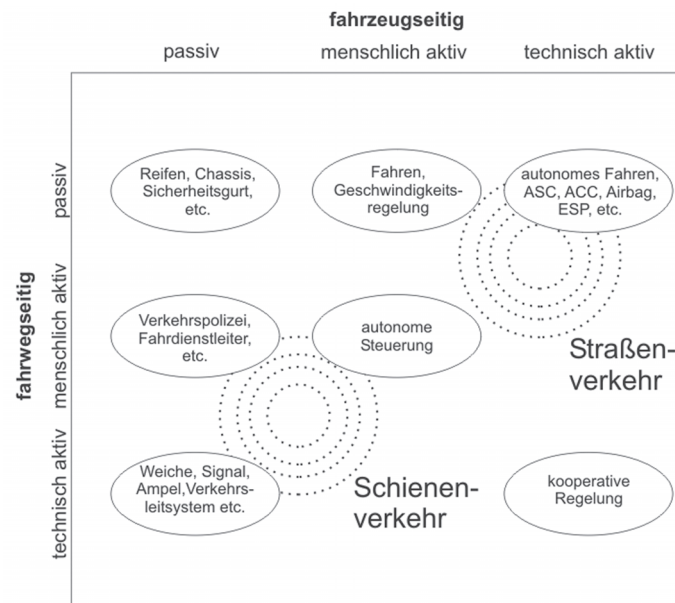


Bild 8: Allokation von Sicherheits- und Steuerungsfunktionen in den Verkehrsbereichen

Der bereits hoch automatisierte und zentral gesteuerte Schienenverkehr, besonders der automatisierte Schienennahverkehr, weist eine hohe Verfügbarkeit und Sicherheit auf. Eine Betrachtung der Bahnübergänge als Beispiel eines multimodalen Bereiches zeigt jedoch ein sehr hohes Risiko, das in den meisten Fällen auf undisziplinierte menschliche Verfehlungen der Autofahrer zurückzuführen und nur durch restriktive Automatisierung reduzierbar ist. Ebenfalls weist die hochprofessionelle Luftfahrt, besonders wenn optimal geschultes Personal involviert ist, eine sehr hohe Verfügbarkeit und Sicherheit auf.

Im Vergleich zum Flug- und Eisenbahnverkehr liegt die Sicherheitsverantwortung im Straßenverkehr in der Hand von unprofessionellen, undisziplinierten und nicht überwachten bzw. überwachbaren Menschen. Wird dort beispielsweise mittels Ausdehnung der fahrwegseitigen und hierarchisch verwalteten Verkehrsregelung ein Anstieg der Sicherheit erzielt, kann zwar daraus gleichzeitig ein Anstieg der Verfügbarkeit resultieren. Für diese Maßnahme müssen neben der Erfüllung drastischer gesetzlicher Anforderungen technische Neuerungen in den Bereichen Statuserkennung, der Feldkommunikation und der Planung/Verfolgung von Trajektorien umgesetzt sowie die Akzeptanz der betroffenen Personen vorausgesetzt werden. Der umgekehrte Ansatz erweist sich allerdings als Erfolg versprechender. So kann ein primär erzielter Anstieg der

Verfügbarkeit gleichzeitig die Sicherheit erhöhen. Ein attraktiver Ansatz kann ein kooperatives und lokal (fahrzeugseitig) ausgeführtes Verkehrsleitsystemkonzept darstellen. Auf Grund von bestehenden marktorientierten Interessen könnte dieser Ansatz auch zu einem Anstieg von Innovationen führen.

Dank

Der Autor dankt Herrn Dipl.-Ing. Jörn Drewes für seine Unterstützung bei der Erstellung dieses Aufsatzes.

Literatur

- [ACKERMANN] ACKERMANN, T (1998), Dissertation: Die Bewertung der Pünktlichkeit als Qualitätsparameter im Schienenpersonenverkehr auf der Basis der direkten Nutzenmessung, Universität Stuttgart.
- [BIKKER] BIKKER, G. & SCHROEDER, M. (2002), Dissertation: Methodische Anforderungsanalyse und automatisierter Entwurf sicherheitsrelevanter Eisenbahnleitsysteme mit kooperierenden Werkzeugen. Technische Universität Braunschweig, VDI-Verlag Düsseldorf.
- [BITSCH] BITSCH, F. (2003), A way for applicable formal specification of safety requirements by tool support, in proceedings: FORMS 2003, Budapest, Hungary.
- [EN 50126] CENELEC–Norm: EN 50126, Railway applications – The specification and demonstration of reliability, availability, maintainability and safety (RAMS), Brussels, 1998.
- [EN 50128] CENELEC–Norm: EN 50128, Railway applications – Software for rail control and monitoring systems, Brussels, 1998.
- [ENGELL] ENGELL, S., G. FREHSE & E. SCHNIEDER (2002): Modelling, Analysis, and Design of Hybrid Systems, Springer LNCIS, ISBN: 3-540-43812-2, Germany.
- [FME] Formal Methods Europe Symposium, (Germany 2001, Denmark 2002, Italy 2003).
- [FORMS] Formal Methods for Railway Operation and Control Systems, (Germany 1998-2004, Hungary 2003).
- [HEILMANN] HEILMANN, K. (2002): Das Risiko der Sicherheit, Hirzel, ISBN: 3-7776-1148-4, Leipzig.
- [IEC 61508] International Standard (1998): Functional safety of electrical/electronic/programmable electronic safety-related systems.

- [KUEHNE] KÜHNE, R. (2004): Ist Mobilität finanzierbar? Verleihung der Carl-Friedrich Gauss Medaille an Prof. Dr. Joachim Milberg, Braunschweigische Wissenschaftliche Gesellschaft.
- [SCHNIEDER99] SCHNIEDER, E. (1999), Methoden der Automatisierung. Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme. Vieweg Verlag, ISBN: 3-528-06566-4
- [SCHNIEDER03] SCHNIEDER, E., (2003), Verlässlichkeit von Verkehrssystemen im Verfügbarkeits-Sicherheits-Diagramm. In: Signal & Draht 10/03.
- [SLOVAK03] SLOVÁK, R., J. MAY & E. SCHNIEDER (2003): PROFUND modelling for holistic risk and availability analysis by means of stochastic Petri nets applied to a level crossing control system. In: Tarnai, G.; Schnieder, E., Hrsg.: Formal Methods for Railway Operation and Control Systems, S. 221-232, Budapest. Symposium FORMS 2003, Budapest, 15.-16.05.2003, L'Harmattan. ISBN 963-9457-45-0.
- [WILTSCHKO] WILTSCHKO, T. (2004): Dissertation: Sichere Information durch infrastrukturgestützte Fahrerassistenzsysteme zur Steigerung der Verkehrssicherheit an Straßenknotenpunkten. Fortschritt-Bericht VDI, Reihe 12, Nr. 570. Düsseldorf: VDI-Verlag.
- [ZASTROW] ZASTROW, K. F. (2000): Dissertation: Analyse und Simulation von Entstörstrategien bei der Automatisierung von U-Bahnsystemen, Technische Universität Berlin.
- [ZHU] ZHU, P. (2001): Dissertation: Betriebliche Leistung von Bahnsystemen unter Störungsbedingungen, Technische Universität Braunschweig, VDI Verlag Düsseldorf.